UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/740,617	12/18/2000	Victor Kouznetsov	002.0181.01	9890

22895 7590 12/30/2004

PATRICK J S INOUYE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER	
KIANERSI, MITRA	
ART UNIT	PAPER NUMBER
2145	

DATE MAILED: 12/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/740,617	**Applicant(s)** KOUZNETSOV ET AL.	
	Examiner Mitra Kianersi	**Art Unit** 2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

Response to Arguments

Applicant's arguments filed Aug/12/2004 have been fully considered but they are not persuasive.

Applicant on page 5, line 1 argues that Nachenberg fails to provide a suggestion or motivation to combine with the reference teachings of Serbinis. Nachenberg on col 5, lines 5-25 disclose that while a "direct action" virus infects other programs as soon as an infected host program is launched, a "memory resident" virus installs itself as a resident interrupt handler and remains dormant until the appropriate interrupt is called. After installing itself as a resident interrupt handler, the memory resident virus returns control to the host program. A dynamic heuristic antivirus program begins emulation at the main entry-point of a target program. However, the infectious viral code (the part of the virus that infects other programs) of a memory resident virus is not reached via the main entry-point of its host program. Instead, the infectious viral code is executed only when the interrupt into which the virus is hooked is called, and a different program other than the infected host program may make such a call to the operating system.
Applicant on page 5, lines 30 argues that Serbinis' reference to scanning documents for viruses does not teach that storing documents is a necessary or desirable part of detecting viruses. Nachenberg on col 1, lines 42-46 disclose that only viruses whose signatures have already been determined and stored in the signature database may be detected using signature scanning. Moreover, the signature database must be updated frequently to detect the latest viruses.
Applicant on page 6, line 25 argues that Nachenberg does not disclose such claim elements as a virus removal sentence and fails to teach or suggest how the actual virus removal should be accomplished. Nachenberg on col 17, lines 43-50 disclose that when a highly suspicious combination generates a false positive by incorrectly identifying a clean program as infected, then that highly suspicious combination may be removed from the list of highly suspicious combinations. Such a list should be quite

robust since more than one highly suspicious combination may be expected to detect a typical virus.

Applicant on page 6, line 27 argues that Nachenberg fails to teach or suggest (1) an identifier uniquely identifying a computer virus. (2) at least one virus name associated with the computer virus, and (3) a virus definition sentence composing object code providing operations to detect the identified computer virus within the computer system. Nachenberg on col 1, lines 39-41 disclose 1) a signature scanning antivirus program can identify particular virus strains for removal and may have a low "false-positive" rate if properly implemented. Nachenberg on col 4, lines 32-34 disclose that 2) some viruses activate only when certain arbitrary conditions are met. For example, consider the pseudo-code of a virus. Nachenberg on col 2, lines 18-26 disclose that 3) non-integrity-based (also called "heuristic") unknown virus detection is used to detect new and unknown viruses without any integrity information. A heuristic antivirus program examines a target program (executable file, boot record, or possibly document file with a macro) and analyzes its program code to determine if the code appears virus-like. If the target program's code appears virus-like, then the possible infection is reported to the user.

Applicant on page 7, lines 5, argues that Serbinis fails to teach or suggest such instructor and also fails to teach or suggest binary data encoding instruction Nachenberg on col 4, lines 32-46 disclose that some viruses activate only when certain arbitrary conditions are met. For example, consider the following pseudo-code of a virus: 1. Find the first file in the current directory that has a ".com" extension (*.com). 2. If a file was found, go to Step 4. 3. Return control to the host program. 4. If the file is less than 1000 bytes long, go to Step 3. 5. If the file name does not end in "EL", go to Step 3. 6. Open the file. Read the first 3 bytes. 8. Seek to the end of the file. 9. Write virus bytes to the file. 10. etc. Also, Serbinis on col 20, lines 66-67 disclose that at step 235, server computer 20 generates two random strings of alphanumeric data, T and K. Because the arguments with respect to the allowableness of independent claims were found unpersuasive, these same arguments are not persuasive with respect to the other dependent claims.

Claims 1-20 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg (US Patent No. 6,357,008) and further in view of Serbinis et al. (US Patent

1. As per claims 1, 10 and 20, Nachenberg disclose a system for distributing portable computer virus definition records with binary file conversion, comprising:

-a structured virus database storing one or more virus definition records, (col 1, lines 27-33) each virus definition record comprising:

-an identifier uniquely identifying a computer virus; (col 1, lines 27-33)

-at least one virus name associated with the computer virus; (col 2, lines 43-44, Unlike virus signatures, these sequences are not designed to be specific to a single virus. Instead, they are meant to be as general as possible in order to detect the operation of many different viruses.

-a virus definition sentence comprising object code providing operations to detect the identified computer virus within a computer system; (col 1, lines 39-41, detected using signature scanning) and

-a virus removal sentence comprising object code providing operations to clean the identified computer virus from the computer system; (col 1, lines 39-41, a signature scanning antivirus program can identify particular virus strains for removal and may have a low "false-positive" rate if properly implemented.

-instructions to clean the computer virus from the computer system; and names associated with the computer virus. (a signature scanning antivirus program can identify particular virus strains for removal and may have a low "false-positive" rate if properly implemented. col 1, lines 39-41)

Nachenburg et al. do not teach a client database engine storing at least one updated virus definition record into the structured virus database indexed by the identifier and the at least one virus name for each virus definition record. However, Serbinis et al. teach a database engine (col 6, lines 27-53) and the at least one name for each definition record (Fig.3, and col 8, lines 12-62, group of objects must be clustered into a definition record with a name, similarly a class of virus can be grouped for executable file, boot record, com. Etc.)

Nachenburg et al. do not teach a converter converting the virus definition records stored in the structured virus database into a virus data file comprising virus definition sets, each virus definition set comprising binary data encoding instructions to detect the computer virus within a computer system. However, Serbinis et al. teach the document may be automatically compressed or encrypted, or at the Originator's request, converted to a particular file format suitable for the Authorized Users (e.g., converted from WordPerfect.RTM. to Microsoft Word). Other forms of filtering may include formatting, translating or virus checking. Both the storage and filtering step, if performed, are logged to the appropriate tables in DMS database. col 10, lines 51-61)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nachenberg et al. with the teachings of Serbinis et al. to include a data base engine accessing the virus definition records in the structured virus database indexed y the identifier and at least one name for each virus definition record because logical collections can be stored at the same time and relationship maintained, col 8, lines 54-57)

2. As per claim 2, Nachenberg disclose a system further comprising:

-a client anti-virus language decompiler converting each virus definition set in the virus data file into a virus definition record. (an anti-virus language compiler is implied as unknown viruses are mapped to code that appears virus like, col 2, lines 18-25) and (col 1, lines 39-45)

3. As per claim 3, Nachenberg disclose a system further comprising a server database engine comparing subsequently modified versions of the structured virus database to form a delta set of virus definition records; (col 7, lines 25-27) and the client database engine storing the delta virus definition records set into the structured virus database. (col 1, lines 27-33)

4. As per claim 4, Nachenberg disclose a system further comprising:
a server database engine building the virus definition records into the structured virus database by generating the identifier for each virus definition record and populating each virus definition record with the virus definition sentence and the virus removal sentence for the computer virus, col 1, lines 39-45)

5. As per claim 5, Nachenberg disclose a system further comprising a server anti-virus language decompiler converting each virus definition set in the virus data file into a virus definition record. (col 2, lines 18-25)

6. As per claim 6, Nachenberg disclose a system further comprising:
-the database engine accessing the virus definition records in the structured virus database (col 1, lines 27-38) to perform at least one of adding, removing, and replacing a virus definition record. (updated database, col 1, lines 44-45)

7. As per claim 7, Nachenberg does not teach a compression module compressing the structured virus database prior to transfer and a decompression module decompressing the structured virus database subsequent to transfer. However, Serbinis et al. teach a compression module compressing the structured virus database prior to transfer (col 11, lines 66-67 and col 12, lines 1-7) and a decompression module decompressing the structured virus database subsequent to transfer (col 13, lines 46-49). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nachenberg et al. with the teachings of Serbinis et al. to include a compression module compressing the structured virus database prior to transfer and a decompression module decompressing the structured virus database subsequent to transfer because it allows documents to be filtered during the retrieval, Serbinis et al. col 13, lines 46-49).

8. As per claim 8, Nachenberg does not teach an encryption module encrypting the structured virus database prior to transfer; and a decryption module decrypting the structured virus database subsequent to transfer. Serbinis et al. teach an encryption module encrypting the structured virus database prior to transfer; (col 11, lines 66-67 and col 12, lines 1-7) and a decryption module decrypting the structured virus database subsequent to transfer.(col 13, lines 46-49). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nachenberg et al. with the teachings of Serbinis et al. to include an encryption module encrypting the structured virus database prior to transfer; and a decryption module decrypting the structured virus database subsequent to transfer because it allows documents to be filtered during the retrieval, Serbinis et al. col 13, lines 46-49).

9. As per claim 9, Nachenberg does not teach a system wherein the structured virus database is a relational database. However, Serbinis et al. teach wherein the structured virus database is a relational database. (col 6, lines 27-53). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nachenberg et al. with the teachings of Serbinis et al. wherein the structured virus database is a relational database because it allows documents to be filtered during the retrieval process then entries may include a storage type, a storage path (i.e. index), a name, a maximum size and a state value (Serbinis et al., col 6, lines 27-53)

10. Claims 11-18 recite the same limitations as claims 2-9. Therefore, they are analyzed and rejected by the same rationale.

11. As per claim 19, Nachenberg does not teach a computer-readable storage medium holding code. (col 3, lines 10-67)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mitra Kianersi whose telephone number is (571) 272-3915. The examiner can normally be reached on 7:00AM-4:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jack Harvey can be reached on (571) 272-3896. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JACK B. HARVEY
SUPERVISORY PATENT EXAMINER

Mitra Kianersi
Dec/30/2004